A. Clifford Edwards
Triel D. Culver
EDWARDS, FRICKLE & CULVER
1648 Poly Drive, Suite 206
Billings, Montana 59102
Telephone: (406) 256-8155
Email: jenny@edwardslawfirm.org
triel@edwardslawfirm.org

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
GREAT FALLS DIVISION

DUSTIN SIEVERS, on behalf of himself and all others similarly situated, Plaintiff, v. EQUIFAX INC., and EQUIFAX INFORMATION SERVICES, LLC, Defendants.	Cause No: **CLASS ACTION COMPLAINT FOR DAMAGES** JURY TRIAL DEMANDED

Plaintiff Dustin Sievers ("Plaintiff" or "Class Representative"), on behalf of himself and the Classes defined below, alleges the following against Equifax Inc. and Equifax Information Services, LLC ("Defendants," "Equifax," or the "Company"), based on personal knowledge as to Plaintiff's conduct and on information and belief as to the acts of others.

I. INTRODUCTION

1. Defendants are one of the three largest consumer credit reporting agencies in the United States. Plaintiff has been a consumer of Equifax's services

and entrusted Defendants with his personal information for many years. He brings this action on a class basis alleging violations of the Fair Credit Reporting Act, Montana's identity theft prevention law, Montana's Consumer Protection Act, negligence, negligence per se, contract claims, unjust enrichment, and bailment, and seeking declaratory relief and redress for affected Equifax consumers.

2. As Plaintiff and the Class entrusted Defendants with their sensitive personal information, Equifax owed them a duty of care to take adequate measures to protect the information entrusted to it, to detect and stop data breaches, and to inform Plaintiff and the Class of data breaches that could expose them to harm. Equifax failed to do so.

3. Equifax acknowledges that, between May 2017 and July 2017, they were the subject of a data breach in which unauthorized individuals accessed Equifax's database and the names, Social Security numbers, addresses, and other Personal Identifying Information ("PII") stored therein (hereinafter the "Data Breach"). According to Equifax, the Data Breach affected as many as 143 million people. Equifax admits that they discovered the unauthorized access on July 29, 2017, but failed to alert Plaintiff and the Class to the fact of the breach until September 7, 2017.

4. The Data Breach was the inevitable result of Equifax's inadequate approach to data security and the protection of the PII that they collected during

the course of their business. Defendants knew and should have known of the inadequacy of their own data security. Equifax has experienced similar such breaches of PII on smaller scales in the past, including in 2013, 2016, and even as recently as January 2017. Over the years, Equifax has jeopardized the PII and, as a result, financial information of hundreds of thousands of Americans.

5. Despite this long history of breaches, Defendants have failed to prevent the Data Breach that has exposed the personal information of over 100 million Americans. The damage done to these individuals may follow them for the rest of their lives, as they will have to monitor closely their financial accounts to detect any fraudulent activity and incur out-of-pocket expenses for years to protect themselves from, and to combat, identity theft now and in the future.

6. Equifax knew and should have known the risks associated with inadequate security, and with delayed reporting of the breach. The potential for harm caused by insufficient safeguarding of PII is profound. With data such as that leaked in the Data Breach, identity thieves can cause irreparable and long-lasting damage to individuals, from filing for loans and opening fraudulent bank accounts to selling valuable PII to the highest bidder.

7. In the case of Defendants' Data Breach, the potential repercussions for consumers are particularly egregious. Privacy researchers and fraud analysts

have called this attack "as bad as it gets." "On a scale of 1 to 10 in terms of risk to consumers," it is a 10.[1]

8. Defendants failed to inform millions of consumers of the Data Breach until September 7, 2017, over a month after Defendants first discovered it on July 29. While Defendants took no steps to inform the public in the interim, Defendants did not hesitate to protect themselves; at least three Equifax senior executives, including CFO John Gamble, upon information and belief, sold shares worth $1.8 million in the days following the Data Breach.[2]

9. To provide relief to the millions of people whose PII has been compromised by the Data Breach, Plaintiff bring this action on behalf of himself and all others similarly situated. Plaintiff seeks to recover actual and statutory damages, equitable relief, restitution, reimbursement of out-of-pocket losses, other compensatory damages, credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Equifax to improve their data security and to bring to an end their long history of breaches at the cost of consumers.

---

[1] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html
[2] https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack

II. THE PARTIES

A. PLAINTIFF

10. Dustin Sievers is an individual consumer, who resides in Wolf Point, Montana. He is currently deployed with the U.S. Military in San Diego. Mr. Sievers engaged, or authorized the engagement of, Equifax at various times over the years, and did so recently in the process of checking his free credit report. As a result, Equifax has possessed his financial history, including his social security number, birthdate, personal addresses, and other sensitive personally identifying information. Mr. Sievers was a victim of the breach. Since the breach, he has spent time monitoring and attempting to protect his credit and accounts from the improper use of his PII obtained by unauthorized third parties as a result of the Data Breach.

B. DEFENDANTS EQUIFAX

11. Defendants are a multi-billion dollar corporation incorporated in Georgia. They provide credit information services to millions of businesses, governmental units, and consumers across the globe. Equifax operates through various subsidiaries and agents, each of which entities acted as agents of Equifax, or in the alternative, in concert with Equifax.

III. JURISDICTION AND VENUE

12. This Court has jurisdiction under 28 U.S.C. § 1332 because there are over 100 Class Members, the amount in controversy exceeds $5 million exclusive of interest and costs, and this is a class action in which many members of the proposed classes, on the one hand, and Defendant, on the other, are citizens of different states.

13. The District of Montana has personal jurisdiction over Defendants because Defendants do business in Montana and in this district; Defendants advertise in a variety of media throughout the United States, including Montana; and many of the acts complained of and giving rise to the claims alleged herein occurred in the District of Montana. Defendant intentionally avails itself of the markets within this state, rendering the exercise of jurisdiction by this Court just and proper.

14. Venue is proper pursuant to 28 U.S.C. Section 1391 because Plaintiff resides in Wolf Point, Defendant conducts substantial business within this division, a substantial part of the events and omissions giving rise to the claims alleged herein occurred in this division, and a substantial part of the property that is the subject of the action is situated in this division.

IV. FACTUAL ALLEGATIONS

15. Equifax has collected and stored personal and credit information from Class members, including Plaintiff.

16. Equifax owed a duty to Plaintiff and the Classes, who entrusted Defendants with their private information, to use reasonable care to protect their PII from unauthorized access by third parties and to detect and stop data breaches, to comply with laws implemented to preserve the privacy of this information, and to notify them promptly if their information was disclosed to an unauthorized third party.

17. Equifax knew or should have known that their failure to meet this duty would cause substantial harm to Plaintiff and the Classes, including serious risks of credit harm and identity theft for years to come.

18. As Equifax was well-aware, or reasonably should have been aware, the PII collected, maintained and stored in its systems is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud. It is well known and the subject of many media reports that PII is highly coveted and a frequent target of hackers. Prior to May 2017, Equifax had experienced at least three major cybersecurity incidents in which consumers' personal information was compromised and accessed by unauthorized third parties.

19. Despite the frequent public announcements of data breaches of corporate entities, including Equifax itself, Equifax maintained an insufficient and inadequate system to protect the PII of Plaintiff and Class members, in breach of their duties to Plaintiff and the Classes. Given the Company's history of cyberattacks and their reputation as an industry leader in data breach security, Equifax could have and should have invested more money and resources into ensuring the security of their data.

20. Because Equifax negligently failed to maintain adequate safeguards, unauthorized third parties managed to exploit a weakness in Equifax's US website application to gain access to sensitive data for roughly two months, beginning in May 2017. The information accessed included names, Social Security numbers, birth dates, addresses, and, in some cases, driver's license numbers. In addition, credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers, were accessed.

21. Equifax was, or reasonably should have been, aware of the vulnerability in their system as early as March 2017. In or about March 2017, Equifax discovered a vulnerability in their U.S. website: Apache Struts CVE-2017-5638. Despite knowing that this system flaw jeopardized the PII of millions of consumers, they failed to implement an effective patch for at least 9 weeks, and

failed to check this known vulnerability regularly to ensure that consumers' information was secure throughout the period of the Data Breach.

22. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiff's and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

23. Equifax delayed informing Plaintiff, the Classes, and the public of the Data Breach. On September 7, 2017, Equifax announced to the public that they had discovered "unauthorized access" to company data, which jeopardized sensitive information for millions of their consumers.

24. At all relevant times, Equifax knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if their data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

25. As a direct, proximate, and foreseeable result of Equifax's failure to meet their duty of care, including by failing to maintain adequate security measures and failing to provide adequate notice of the Data Breach, Plaintiff and the Classes

have suffered and will continue to suffer substantial harm, including inconvenience, distress, injury to their rights to the privacy of their information, increased risk of fraud, identity theft, and financial harm, the costs of monitoring their credit to detect incidences of this, and other losses consistent with the access of their PII by unauthorized sources.

26. Armed with the stolen information, unauthorized third parties now possess keys that unlock consumers' medical histories, bank accounts, employee accounts, and more. Abuse of sensitive credit and personal information can result in considerable harm to victims of security breaches. Criminals can take out loans, mortgage property, open financial accounts and credit cards in a victim's name, obtain government benefits, file fraudulent tax returns, obtain medical services, and provide false information to police during an arrest, all under the victim's name. Furthermore, this valuable information can also be sold to others with similar nefarious intentions.

27. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including,

inter alia, by placing “freezes” and “alerts” with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency’s slippage, as is the case here.

28. A breach of this scale requires Plaintiff and Class members to incur the burden of scrupulously monitoring their financial accounts and credit histories to protect themselves against identity theft and other fraud and will spend time and incur out-of-pocket expenses to protect against such theft. This includes obtaining credit reports, enrolling in credit monitoring services, freezing lines of credit, and more. Where identity theft is detected, Plaintiff and Class members will incur the burden of correcting their financial records and attempting to correct fraud on their accounts, to the extent that that is even possible. Plaintiff and Class members will likely spend considerable effort and money for the rest of their lives on monitoring and responding to the repercussions of this cyberattack.

29. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;
b. unauthorized charges on their debit and credit card accounts;
c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiff's and Class members' information on the black market;
d. the untimely and inadequate notification of the Data Breach;
e. the improper disclosure of their PII;
f. loss of privacy;
g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;
h. ascertainable losses in the form of deprivation of the value of their PII,
i. for which there is a well-established national and international market;

j. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

k. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and,

l. the loss of productivity and value of their time spent to attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

30. Because Equifax has demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and members of the Classes have an undeniable interest in insuring that their PII, which remains in

Equifax's possession, is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

V. CLASS ACTION ALLEGATIONS

31. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23 seeking injunctive and monetary relief for Equifax's systemic failure to safeguard personal information of Plaintiff and Class members.

A. CLASS DEFINITIONS

32. Plaintiff seeks relief in his individual capacity and as a representative of all others who are similarly situated.

33. The "Nationwide Class" is defined as all persons residing in the United States whose personal data Equifax collected and stored and whose personal information was placed at risk and/or disclosed in the Data Breach affecting Equifax from May to July 2017.

34. The "Montana Class" is defined as all persons residing in Montana whose personal data Equifax collected and stored and whose personal information was placed at risk and/or disclosed in the Data Breach affecting Equifax from May to July 2017.

35. Excluded from either class are all attorneys for the class, officers, and members of Equifax, including officers and members of any entity with an

ownership interest in Equifax, any judge who sits on this case, and all jurors and alternate jurors who sit on this case.

36. Except where otherwise noted, "Class members" shall refer to members of the Nationwide Class and of the Montana Class collectively.

37. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

B. REQUIREMENTS OF RULE 23(a) AND RULE 23(b)(2) and (b)(3)

i. Numerosity and Impracticability of Joinder

38. The proposed Classes are so numerous that joinder of all members is impracticable.

39. Upon information and belief, there are more than 143 million members of the proposed Nationwide Class, and hundreds of thousands of members in the Montana Class.

40. The Class members are readily ascertainable. Equifax has access to information about the Data Breach, the time period of the Data Breach, and which individuals were affected. Using this information, the members of the Class can be identified and their contact information ascertained for purposes of providing notice.

ii. Common Questions of Law and Fact

41. Every Class member suffered injuries as alleged in this complaint as a result of Defendants' misconduct. The prosecution of Plaintiff's claims will require the adjudication of numerous questions of law and fact common to the Classes. The common questions of law and fact predominate over any questions affecting only individual Class members. The common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants owed a duty to Plaintiff and Class Members to adequately protect their personal information;

c. Whether Defendants breached their duties to protect the personal information of Plaintiff and Class members;

d. Whether Defendants knew or should have known that their data security systems and processes were unreasonably vulnerable to attack;

e. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of personal information; and

f. Whether Plaintiff and Class members are entitled to equitable relief including injunctive relief.

iii. Typicality of Claims and Relief Sought

42. Plaintiff has suffered the same violations and similar injuries as other Class members arising out of and caused by Defendants' common course of conduct. All Class members were subject to the same acts and omissions by Defendants, as alleged herein, resulting in the breach of personal information.

43. Plaintiff possesses and asserts each of the claims on behalf of the proposed Classes. He seeks similar relief as other Class members.

iv. Adequacy of Representation

44. Plaintiff's interests are coextensive with those of the members of the proposed Classes. Each suffered risk of loss and credit harm and identity theft caused by Equifax's wrongful conduct and negligent failure to safeguard their data, the injuries suffered by Plaintiff and the Class members are identical (i.e. the costs to monitor and repair their credit through a third-party service), and Plaintiff's claims for relief are based upon the same legal theories as are the claims of the other Class members. Plaintiff is willing and able to represent the proposed Classes fairly and vigorously.

45. Plaintiff has retained counsel sufficiently qualified, experienced, and able to conduct this litigation and to meet the time and fiscal demands required to litigate a class action of this size and complexity.

v. Efficiency of Class Prosecution of Class Claims

46. A class action is superior to other available methods for the fair and efficient adjudication of the controversy – particularly where individual class members lack the financial resources to vigorously prosecute a lawsuit against a large corporation such as Equifax.

47. Class action treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of efforts and expense that numerous individual actions engender.

48. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent and/or varying adjudications with respect to the individual members of the Classes, establishing incompatible standards of conduct for Defendants and resulting in the impairment of Class members' rights and the disposition of their interests through actions to which they were not parties.

49. The issues in this class action can be decided by means of common, classwide proof. In addition, the Court can, and is empowered to, fashion methods to efficiently manage this action as a class action.

C. Requirements of Rule 23(b)(2)

50. Equifax has acted or refused to act on grounds generally applicable to Plaintiff and the proposed Classes by failing to take necessary steps to safeguard Plaintiff's and Class members' personal information.

51. Equifax's systemic conduct justifies the requested injunctive and declaratory relief with respect to the Classes.

52. Injunctive, declaratory, and affirmative relief are predominant forms of relief sought in this case. Entitlement to declaratory, injunctive, and affirmative relief flows directly and automatically from proof of Equifax's failure to safeguard consumers' personal information. In turn, entitlement to declaratory, injunctive, and affirmative relief forms the factual and legal predicate for the monetary and non-monetary remedies for individual losses caused by Equifax's failure to secure such information.

D. Rule 23(c)(4) Issue Certification

53. Additionally, or in the alternative, the Court may grant "partial" or "issue" certification under Rule 23(c)(4). Resolution of common questions of fact and law would materially advance the litigation for all Class members.

VI. COUNTS

COUNT I

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

(On behalf of the Nationwide and Montana Classes)

54. Plaintiff incorporates all preceding and subsequent paragraphs by reference.

55. Plaintiff and Class members are consumers entitled to the protections of the Fair Credit Reporting Act, 15 U.S.C. § 1681a(c) (“FCRA”).

56. Under the FCRA, a “consumer reporting agency” is defined as “any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties . . .” 15 U.S.C. § 1681a(f).

57. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, they regularly engage in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

58. As a consumer reporting agency, the FCRA requires Equifax to “maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title.” 15 U.S.C. § 1681e(a).

59. Under the FCRA, a “consumer report” is defined as “any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of

serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. § 1681a(d)(1). The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

60. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed the Class members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

61. Equifax furnished Class members' consumer reports by disclosing their consumer reports to unauthorized entities and computer hackers; allowing unauthorized entities and computer hackers to access their consumer reports; knowingly and/or recklessly failing to take security measures that would prevent

unauthorized entities or computer hackers from accessing their consumer reports; and/or failing to take reasonable security measures that would prevent unauthorized entities or computer hackers from accessing their consumer reports.

62. The Federal Trade Commission ("FTC") has pursued enforcement actions against consumer reporting agencies under the FCRA for failing to "take adequate measures to fulfill their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

63. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under § 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, Equifax's numerous other data breaches in the past. Further, Defendants tout themselves as industry leaders in breach prevention; thus, they were well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

64. Defendants also acted willfully and recklessly because they knew or should have known about their legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission.

Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiff and other members of the Classes of their rights under the FCRA.

65. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiff's and the Class members' PII for no permissible purposes under the FCRA.

66. Plaintiff and the Class members have been damaged by Equifax's willful or reckless failure to comply with the FCRA. Therefore, Plaintiff and each of the Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

67. Plaintiff and the Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

COUNT II

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

(On behalf of the Nationwide and Montana Classes)

68. Plaintiff incorporates all preceding and subsequent paragraphs by reference.

69. Equifax was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under § 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

70. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiff's and Class members' PII and consumer reports for no permissible purposes under the FCRA.

71. Plaintiff and the Class members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiff and each of the Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

72. Plaintiff and the Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT III

VIOLATION OF MONTANA'S IDENTITY THEFT PREVENTION LAW

(On behalf of the Montana Class)

73. Plaintiff incorporates all preceding and subsequent paragraphs by reference.

74. Plaintiff and the Montana Class members are "customers" under Mont. Code Ann. § 30-14-1702.

75. Under Mont. Code Ann. § 30-14-1704, a "business that conducts business in Montana and that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the data system following discovery or notification of the breach to any resident of Montana whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person […] without unreasonable delay […]."

76. Similarly, a "business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data system immediately following discovery if the personal information was or is reasonably believed to have been acquired by an unauthorized person." Mont. Code Ann. § 30-14-1704.

77. Moreover, "[a] business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer necessary to be retained by the

business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable." Mont. Code Ann. § 30-14-1703.

78. Equifax is a business that conducts business in Montana and that owns or licenses computerized data that includes personal information.

79. In the alternative, Equifax is a business that maintains computerized data that includes personal information that the business does not own.

80. The Data Breach is a "Breach of the security of the data system" because it included names in combination with social security numbers, credit card information, and, in some instances, driver's license numbers.

81. Plaintiff's and the Montana Class members' PII (including but not limited to names, addresses, and Social Security numbers) includes personal information.

82. Equifax violated Mont. Code Ann. § 30-14-1704 by failing to disclose the Data Breach without unreasonable delay, or, in the alternative, immediately, to Plaintiff and Montana Class members.

83. Equifax violated Mont. Code Ann. § 30-14-1703 by failing to take reasonable steps to destroy or modify Plaintiff's and Montana Class members' PII to make it unreadable or undecipherable after it was no longer necessary to any service Defendants provide.

84. As a direct and proximate result Equifax's violations of Mont. Code Ann. § 30-14-1703 and Mont. Code Ann. § 30-14-1704, Plaintiff and the Montana Class members suffered the damages alleged herein.

85. Plaintiff and Montana Class members are entitled to damages to be proved at trial, including, but not limited to actual damages and attorneys' fees.

86. This claim is asserted in the alternative, and to the extent that Equifax is not subject to any exception from these laws.

COUNT IV

VIOLATION OF MONTANTA'S CONSUMER PROTECTION ACT - MONT. CODE ANN. 30-14-101 ET SEQ.

(On Behalf of the Montana Class)

87. Plaintiff incorporates all preceding and subsequent paragraphs by reference.

88. Plaintiff and the Montana Class members are "consumers" under Mont. Code Ann. § 30-14-102.

89. Montana's Consumer Protection Act (the "MCPA") prohibits Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. Mont. Code Ann. § 30-14-103.

90. Any action prohibited in section 5(a)(1) of the FCT Act is also a violation of the MCPA. Mont. Code Ann. § 30-14-104; Mont.Admin.R. 23.19.101.

91. Equifax, while operating in Montana, engaged in unfair and deceptive acts or practices, in violation of Mont. Code Ann. § 30-14-103. Equifax's unfair and deceptive practices include but are not limited the following:

a. Equifax failed to enact adequate privacy and security measures to protect the Montana Class members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Equifax failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Equifax knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the Montana Class members' PII from unauthorized disclosure, release, data breaches, and theft;

d. Equifax knowingly omitted, suppressed, and concealed the inadequacy of their privacy and security protections for Montana Class members' PII;

e. Equifax knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Montana Class members' PII, including but not limited to duties imposed by the FCRA, 15. U.S.C.§ 1681e, the FTC Act, the GLBA, 15 U.S.C. § 6801 et seq., Mont. Code Ann § 30-14-1703, and Mont. Code Ann § 30-14-1704;

f. Equifax failed to maintain the privacy and security of the Montana Class members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, which was a direct and proximate cause of the Data Breach;

g. Equifax failed to disclose the Data Breach to the Montana Class members in a timely and accurate manner, in violation of Mont. Code Ann § 30-14-1704; and

h. Equifax failed to take reasonable steps to destroy or modify Plaintiff's and Montana Class members' PII to make it unreadable or undecipherable after it was no longer necessary to any service Defendants provide.

92. Plaintiff and Montana Class members have suffered the ascertainable losses described herein. These include the loss of the property interest in their private PII as a result of Equifax's violation of Mont. Code Ann. § 30-14-103. Plaintiff and Class members have also suffered ascertainable monetary losses or

are at imminent risk of monetary losses, as a result of Equifax's violation of Mont. Code Ann. § 30-14-103.

93. The Court is empowered to order restoration of money and property lost as a result of Defendant's violations of the MCPA. Each Named Plaintiff and each member of the Montana Class entitled to receive the greater of actual damages or $500. The Court may, in its discretion, award up to three times the actual damages sustained and may provide any other equitable relief that it considers necessary or proper. Plaintiff is entitled to reasonable attorneys' fees.

COUNT V

NEGLIGENCE

(On Behalf of Nationwide and Montana Classes)

94. Plaintiff incorporates all preceding and subsequent paragraphs by reference.

95. Equifax owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class members' information adequately secured from unauthorized access.

96. Equifax owed a duty to Class members to implement intrusion detection processes that would detect a data breach in a timely manner.

97. Equifax also had a duty to delete any PII that was no longer needed to serve client needs.

98. Equifax owed a duty to disclose the material fact that their data security practices were inadequate to safeguard Class Members' PII.

99. Equifax also had independent duties under federal and state laws that required Equifax to reasonably safeguard Plaintiff's and Class members' PII and promptly notify them about the Data Breach.

100. Equifax had a special relationship with Plaintiff and Class members from being entrusted with their PII, which provided an independent duty of care. Moreover, Equifax had the ability to protect their systems and the PII they stored on them from attack.

101. Equifax breached their duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class Members' PII; (b) failing to detect and end the Data Breach in a timely manner; (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' PII; and (d) failing to provide adequate and timely notice of the breach.

102. But for Equifax's breach of their duties, Class Members' PII would not have been accessed by unauthorized individuals.

103. Plaintiff and Class members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of their data security systems would cause damages to Class members.

104. Equifax engaged in this misconduct recklessly, in conscious neglect of duty and in callous indifference to consequences, and, in the alternative, with such want of care as would raise a presumption of a conscious indifference to consequences. Equifax was or should reasonably have been, aware of their misconduct and of the foreseeable injury that would probably result, and with reckless indifference to consequences, consciously and intentionally committed the wrongful acts and omissions herein. Equifax's actions and omissions were, therefore, not just negligent, but grossly negligent, reckless, willful, and wanton.

105. As a result of Equifax's negligence, Plaintiff and Class members suffered and will continue to suffer injury, which includes but is not limited to the monetary difference between the amount paid for services as promised and the services actually provided by Defendants (which did not include adequate or industry standard data protection), inconvenience and exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports,

credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII has also diminished the value of the PII. Plaintiff and the Classes have also experienced other damages consistent with the theft of their PII. Through their failure to timely discover and provide clear notification of the Data Breach to consumers, Equifax prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their PII.

106. The damages to Plaintiff and the Class members were a direct, proximate, reasonably foreseeable result of Equifax's breaches of their duties.

107. Therefore, Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

COUNT VI

NEGLIGENCE PER SE

(On behalf of the Nationwide and Montana Classes)

108. Plaintiff incorporates all preceding and subsequent paragraphs by reference.

109. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII.

110. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Equifax's conduct was particularly unreasonable given the nature and amount of PII they obtained and stored, and the foreseeable consequences of a data breach at a corporation such as Equifax, including, specifically, the immense damages that would result to Plaintiff and Class members.

111. Equifax's violation of Section 5 of the FTC Act constitutes negligence per se.

112. Equifax also violated the FCRA, as stated in Counts I and II. Equifax's violation of the FCRA constitutes negligence per se.

113. The Gramm-Leach-Bliley Act ("GLBA") requires covered entities to satisfy certain standards relating to administrative, technical, and physical safeguards:

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

> (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

15 U.S.C. § 6801(b).

114. Businesses subject to the GLBA "should take preventative measures to safeguard customer information against attempts to gain unauthorized access to the information." Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F.

115. In order to satisfy their obligations under the GLBA, Equifax was required to "develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." See 16 C.F.R. § 314.3; *see also* Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F. (Subject companies must "design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the […] company's activities"). This obligation included considering and, where the Company determined appropriate, adopting mechanisms for "[e]ncryption of electronic customer information, including while

in transit or in storage on networks or systems to which unauthorized individuals may have access." *Id.*

116. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to "develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems." *See id.* "The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities." *Id.*

117. Equifax had an "affirmative duty to protect their customers' information against unauthorized access or use." *Id.* Timely notification of customers in the event of a data breach is key to meeting this affirmative obligation. Accordingly, when Equifax became aware of "unauthorized access to sensitive customer information," they should have "conduct[ed] a reasonable investigation to promptly determine the likelihood that the information has been or will be misused" and "notif[ied] the affected customer[s] as soon as possible." *See id.* Sensitive customer information includes much of the PII released in the Data Breach.

118. Equifax violated the GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and

complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, (a) Equifax's failure to implement and maintain adequate data security practices to safeguard Class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class members' PII.

119. Equifax also violated the GLBA by failing to notify affected customers as soon as possible after they became aware of unauthorized access to sensitive customer information.

120. Equifax's violations of the GLBA constitute negligence per se.

121. Equifax also violated Montana's data breach laws, as stated in Count III. Equifax's violations of Montana's data breach law constitute negligence per se.

122. Equifax also violated the MCPA, as stated in Count IV. Equifax's violations of the MCPA constitute negligence per se.

123. Plaintiff and Class members are within the class of persons that the FTC Act, the FCRA, the GLBA, Montana's data breach laws, and the MCPA were intended to protect.

124. Plaintiff and Class members were foreseeable victims of Equifax's violation of the FTC Act, the FCRA, the GLBA, Montana's data breach laws and

the MCPA. Equifax knew or should have known that their failure to take reasonable measures to prevent a breach of their data security systems, and failure to timely and adequately report it to Class members themselves would cause damages to Class members.

125. The harm that occurred as a result of the Equifax Data Breach is the type of harm the FTC Act, the FCRA, the GLBA, Montana's Identity Theft Prevention law and the MCPA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as suffered by Plaintiff and the Class.

126. Equifax engaged in this misconduct recklessly, in conscious neglect of duty and in callous indifference to consequences, and, in the alternative, with such want of care as would raise a presumption of a conscious indifference to consequences. Equifax was, or should reasonably have been, aware of their misconduct and of the foreseeable injury that would probably result, and with reckless indifference to consequences, consciously and intentionally committed the wrongful acts and omissions herein. Equifax's actions and omissions were, therefore, not just negligent, but grossly negligent, reckless, willful, and wanton.

127. As a direct and proximate result of Equifax's negligence *per se*, Plaintiff and Class members suffered and will continue to suffer injury, which

includes but is not limited to the monetary difference between the amount paid for services as promised and the services actually provided by Defendants (which did not include adequate or industry standard data protection), inconvenience and exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII has also diminished the value of the PII. Plaintiff and the Classes have also experienced other damages consistent with the theft of their PII. Through their failure to timely discover and provide clear notification of the Data Breach to consumers, Equifax prevented Plaintiff and Class members from taking meaningful, proactive steps to secure their PII.

128. But for Equifax's violation of the applicable laws and regulations, Class members' PII would not have been accessed by unauthorized individuals.

129. The damages to Plaintiff and the Class members were a direct, proximate, reasonably foreseeable result of Equifax's breaches of the applicable laws and regulations.

130. Therefore, Plaintiff and Class members are entitled to damages in an amount to be proven at trial.

COUNT VII

BREACH OF IMPLIED CONTRACT

(On behalf of the Nationwide and Montana Classes)

131. Plaintiff incorporates all preceding and subsequent paragraphs by reference.

132. As a necessary prerequisite to obtaining the services Equifax provides, Plaintiff and the Class members provided PII to Defendants.

133. Plaintiff and the Class members also disclosed such information for the benefit of Defendants.

134. The provision of PII by Plaintiff and the Class members, and Defendants' acceptance of such information, created an implied contract whereby Defendants had a duty to safeguard and protect the information of Plaintiff and Class members, consistent with industry standards for PII protection.

135. Equifax did not safeguard or protect Plaintiff's and the Classes' PII from being accessed, compromised, and/or stolen. Defendants did not maintain sufficient security measures and procedures to prevent unauthorized access to Plaintiff's and the Classes' PII and did not provide timely notice of the Data

Breach. Defendants did not comply with the industry standards for the protection of PII.

136. Because Equifax failed to safeguard and/or protect Plaintiff's and the Classes' PII from being compromised or stolen, and failed to comply with industry standards for the protection of such information, Defendants breached their implied contracts with Plaintiff and Class members.

137. Equifax's failure to fulfill its implied contractual obligation to protect PII resulted in Plaintiff and the Class members receiving services of less value than what was promised, i.e., services that included adequate protection of confidential data. Accordingly, Plaintiff and the Class members did not receive the full benefit of their bargain.

138. As a result of Equifax's breach of its implied contract with Plaintiff and Class members, Plaintiff and Class Members suffered and will continue to suffer injury, which includes but is not limited to the monetary difference between the amount paid for services as promised and the services actually provided by Defendants (which did not include adequate or industry standard data protection), inconvenience and exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-

of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Members' PII has also diminished the value of the PII. Plaintiff and the Classes have also experienced other damages consistent with the theft of their PII. Through its failure to timely discover and provide clear notification of the Data Breach to consumers, Equifax prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

COUNT VIII

UNJUST ENRICHMENT

(On behalf of the Nationwide and Montana Classes)

139. Plaintiff incorporates all preceding and subsequent paragraphs by reference.

140. Equifax received payment to perform services that included protecting Plaintiff and the Class members' PII. Equifax failed to do this, but retained Plaintiff's and the Class members' payments.

141. Equifax retained the benefit of said payments under circumstances which rendered it inequitable and unjust for them to retain such benefits without paying for their value.

142. Defendants' retention of this money is without justification because, had Plaintiff and the Class members been aware of the truth of Defendants' misrepresentations and omissions regarding the security of their PII, they would not have utilized their services.

143. Defendants have knowledge of said benefits.

144. Plaintiff and Class members are entitled to recover damages in an amount to be proven at trial.

COUNT IX

BAILMENT

(On behalf of the Nationwide and Classes)

145. Plaintiff incorporates all preceding and subsequent paragraphs by reference.

146. Plaintiff and Class members delivered their PII to Defendants in order to receive services from Defendants.

147. The PII was furnished Defendants for the exclusive purpose of receiving the services Equifax provides in the ordinary course of business, and Defendants took possession of the PII for the same reason.

148. Upon delivery, Plaintiff and Class members intended and understood that Equifax would adequately safeguard their PII, and Defendants, in accepting possession, understood the expectations of Plaintiff and Class members.

Accordingly, bailment was established for the mutual benefit of the parties at the time of delivery and acceptance of possession.

149. Pursuant to the bailment arrangement, Defendants owed Plaintiff and Class members a duty of reasonable care in safeguarding and protecting their PII.

150. Equifax breached this duty by failing to take adequate steps to protect the PII entrusted to them and by failing to conform to best practices and industry standards to prevent unauthorized access to Plaintiff's and Class members' PII.

151. As a result of Equifax's failure to fulfill its bailment arrangement, Plaintiff and Class Members suffered and will continue to suffer injury, which includes but is not limited to the monetary difference between the amount paid for services as promised and the services actually provided by Defendants (which did not include adequate or industry standard data protection), inconvenience and exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiff and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiff's and Class Member's PII has also diminished the value of the PII. Plaintiff and the Classes have also experienced other damages consistent with the

theft of their PII. Through its failure to timely discover and provide clear notification of the Data Breach to consumers, Equifax prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII.

COUNT X

DECLARATORY JUDGMENT

(On behalf of the Nationwide and Montana Classes)

152. Plaintiff incorporates all preceding and subsequent paragraphs by reference.

153. As previously alleged, Plaintiff and Class members entered into an implied contract that required Equifax to provide adequate security for the PII they collected. As previously alleged, Defendants owe duties of care to Plaintiff and Class members that require them to adequately secure PII.

154. Equifax still possesses PII pertaining to Plaintiff and Class members.

155. Equifax has made no announcement or notification that they have remedied the vulnerabilities in their computer data systems.

156. Accordingly, Equifax has not satisfied their obligations and legal duties to Plaintiff and Class members. In fact, now that Equifax's lax approach towards data security has become public, the PII in their possession is more vulnerable than previously.

157. Actual harm has arisen in the wake of the Equifax Data Breach regarding Equifax's contractual obligations and duties of care to provide data security measures to Plaintiff and Class members.

158. Plaintiff, therefore, seeks a declaration that (a) Equifax's existing data security measures do not comply with their contractual obligations and duties of care, and (b) in order to comply with their contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training their security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for their provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating their customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves.

VII. PRAYER FOR RELIEF ON INDIVIDUAL AND CLASS ACTION CLAIMS

WHEREFORE, the Plaintiff and Class Representative, on his own behalf and on behalf of the respective Classes, prays that this Court:

159. Certify this case as a class action maintainable under Federal Rules of Civil Procedure Rule 23(a), (b)(2) and/or (b)(3), on behalf of the proposed Classes; designate the proposed Class Representative as representative; and designate Plaintiff's counsel of record as Class Counsel for each Class;

160. Declare and adjudge that Defendants' policies, practices, and/or procedures challenged herein are illegal and in violation of the rights of the Plaintiff, Class Representatives, and members of the Nationwide and Montana Classes.

161. Issue a permanent injunction against Defendants and their partners, officers, trustees, owners, employees, agents, attorneys, successors, assigns, representatives, and any and all persons acting in concert with them from engaging in any conduct violating the rights of Plaintiff, Class Representatives, members of the Nationwide and Montana Classes, and those similarly situated as secured by law.

162. Order injunctive relief requiring Defendants to (1) strengthen their data security systems that maintain PII to comply with the applicable state laws alleged herein and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendant's systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

163. Award compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement to Plaintiff, Class Representatives, and members of the Classes, in an amount to be determined at trial.

164. Award punitive damages under Montana Code Ann. § 27-1-221 to Plaintiff, Class Representatives, and members of the Classes, in an amount to be determined at trial.

165. Order Defendants to make whole the Plaintiff, Class Representatives, and members of the Classes by providing them with any other monetary and affirmative relief;

166. Order Defendants to pay all costs associated with Class notice and administration of Class-wide relief;

167. Award litigation costs and expenses, including, but not limited to, reasonable attorneys' fees, to the Plaintiff, Class Representatives, and members of the Nationwide and Montana Classes;

168. Award Plaintiff, Class Representatives, and members of the Nationwide and Montana Classes all pre-judgment interest and post-judgment interest available under law;

169. Award Plaintiff, Class Representatives, and members of the Nationwide and Montana Classes any other appropriate equitable relief;

170. Order that this Court retain jurisdiction of this action until such time as the Court is satisfied that the Defendants have remedied the practices complained of herein and are determined to be in full compliance with the law; and

171. Award additional and further relief as this Court may deem just and proper.

VIII. JURY DEMANDED

Plaintiff demands a trial by jury on all issues triable of right by jury.

DATED this 22nd day of September, 2017.

EDWARDS, FRICKLE & CULVER

/s/ Triel D. Culver
A. Clifford Edwards
Triel D. Culver
Attorneys for Plaintiff and the Classes

Ed Chapin (CA SBN 53287, *Pro Hac Vice* forthcoming)
SANFORD HEISLER SHARP, LLP
655 West Broadway, Suite 1700
San Diego, CA 92101
echapin@sanfordheisler.com
Telephone: (619) 577-4253
Facsimile: (619) 577-4250

Kevin Sharp (TN SBN 016287, *Pro Hac Vice* forthcoming)
SANFORD HEISLER SHARP, LLP
611 Commerce St., Suite 3100
Nashville, TN 37203
ksharp@sanfordheisler.com
Telephone: (615) 434-7001
Facsimile: (615) 434-7020

Danielle Fuschetti (CA SBN 294064,
Pro Hac Vice forthcoming)
SANFORD HEISLER SHARP, LLP
111 Sutter Street, Suite 975
San Francisco, CA 94104
dfuschetti@sanfordheisler.com
Telephone: (415) 795-2020
Facsimile: (415) 795-2021

Attorneys for Plaintiff and the Classes